

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2003年11月13日 (13.11.2003)

PCT

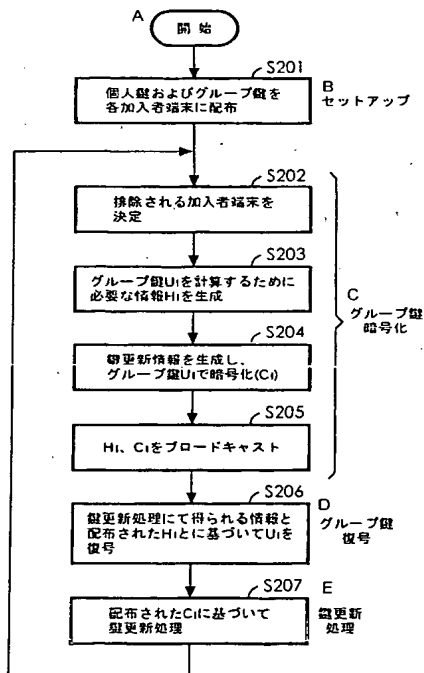
(10) 国際公開番号  
WO 03/094422 A1

- (51) 国際特許分類<sup>7</sup>: H04L 9/08 (72) 発明者: および  
(21) 国際出願番号: PCT/JP03/05482 (75) 発明者/出願人 (米国についてのみ): 渡邊 裕治 (WATANABE, Yuji) [JP/JP]; 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kanagawa (JP). 沼尾 雅之 (NUMAO, Masayuki) [JP/JP]; 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kanagawa (JP).  
(22) 国際出願日: 2003年4月28日 (28.04.2003)  
(25) 国際出願の言語: 日本語  
(26) 国際公開の言語: 日本語  
(30) 優先権データ: 特願2002-129359 2002年4月30日 (30.04.2002) JP  
(71) 出願人 (米国を除く全ての指定国について): インターナショナル・ビジネス・マシーンズ・コーポレーション (INTERNATIONAL BUSINESS MACHINES CORPORATION) [US/US]; 10504 ニューヨーク州 アーモンク ニューオーチャード ロード NY (US).  
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI,

[続葉有]

(54) Title: ENCRYPTED COMMUNICATION SYSTEM, KEY DELIVERY SERVER THEREOF, TERMINAL DEVICE, AND KEY SHARING METHOD

(54) 発明の名称: 暗号通信システム、その鍵配布サーバ、端末装置及び鍵共有方法



A...START  
B...SETUP  
C...GROUP KEY ENCRYPTION  
D...GROUP KEY DECODING  
E...KEY UPDATING  
S201...DELIVER INDIVIDUAL KEY AND GROUP KEY TO SUBSCRIBER TERMINALS  
S202...DECIDE SUBSCRIBER TERMINALS TO BE EXCLUDED  
S203...CREATE INFORMATION H<sub>1</sub> REQUIRED FOR CALCULATING GROUP KEY U<sub>1</sub>  
S204...CREATE KEY UPDATING INFORMATION AND ENCRYPT (C<sub>1</sub>) IT WITH GROUP KEY U<sub>1</sub>  
S205...BROADCAST H<sub>1</sub>, C<sub>1</sub>  
S206...DECODE U<sub>1</sub> ACCORDING TO THE INFORMATION OBTAINED BY KEY UPDATING AND H<sub>1</sub> DELIVERED  
S207...UPDATE KEY ACCORDING TO C<sub>1</sub> DELIVERED

(57) Abstract: A method for providing a highly-safe and high-speed group key updating method. The method includes a step of executing a part of decoding processing for decoding an encrypted group key used for information decoding in a subscriber terminal before delivery of the group

[続葉有]

BEST AVAILABLE COPY

WO 03/094422 A1



NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR),

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

key, a step of delivering the group key and individual decoding information for each terminal device for executing a part of the remaining part of the decoding processing of the group key, and a step of executing in the subscriber terminal a group key decoding processing using the delivered decoding information and the result of the part of the decoding processing executed in advance

(57) 要約: 安全性が高く高速なグループ鍵の更新方法を提供する方法である。情報の復号に用いる暗号化されたグループ鍵を復号するための復号処理の一部が、このグループ鍵の配布前に、加入者端末において実行されるステップと、グループ鍵とこのグループ鍵の復号処理の残りの一部を実行するための端末装置ごとに個別の復号情報とが、加入者端末に配布されるステップと、配布された復号情報と事前に実行された復号処理の一部の結果とを用いたグループ鍵の復号処理が、加入者端末において実行されるステップとを含む。

## 明細書

暗号通信システム、その鍵配布サーバ、端末装置及び鍵共有方法

## 5 技術分野

本発明は、暗号化された情報を復号するための鍵を加入者端末に配布する技術に関し、特に鍵の更新を安全かつ高速に行う技術に関する。

## 10 背景技術

予め決められたグループに対して情報を提供するようなシステムを構築する際に、グループ加入者だけに鍵（グループ鍵）を配布して、その鍵を用いた暗号通信を行う場面が多く登場する。例えば、携帯電話に対するコンテンツ配信、DVDの復号再生器、  
15 C D R O Mによるソフトウェア配信、警察無線、P 2 Pサービスにおけるグループ内通信など、広い応用分野がある。

このようなシステムにおいて、一部の端末装置（復号器）が盗難等により紛失された場合、グループ加入者以外にグループ鍵が漏洩してしまうおそれがある。このため、古いグループ鍵を更新  
20 して、一刻も早く新しいグループ鍵を共有しなければならない。

この鍵更新技術は、一度作られたインフラを長期間利用するようなシステムにおいて、極めて重要な意味を持つ。

複数の加入者端末から構成されるこの種のシステム（以下、放  
25 送型暗号通信システム）において、任意に決定した単数または複数の加入者端末を除く全加入者端末に対してメッセージを配布することを考える。ここで、ある加入者端末をグループから除くことを「排除する」、その加入者端末を「排除対象端末」と呼ぶ。一般に、排除対象端末を排除するには、排除対象端末以外の個々の加入者  
30 の加入者端末に新たなグループ鍵を配送する必要がある。そのため、グループの規模の拡大に伴い、通信量や全加入者端末間で新しいグループ鍵の共有が完了するまでの遅延が増加する。

従来、上述したグループ鍵の更新の際における遅延を減少させるため、種々の方法が検討されている。この種の従来技術としては、例えば特開 2 0 0 0 - 1 9 6 5 8 1 号公報に開示された技術  
5 がある（従来技術 1）。

同公報に開示された従来技術 1 は、排除対象端末が決定後の通信量や遅延がグループ加入者総数  $n$  に比例しない手法が用いられている。この手法では、排除対象端末の最大数を  $k$  であるとする  
10 と、各加入者端末がグループ鍵を計算するために、 $k$  に比例した冪剰余演算が必要になる。したがって、 $k$  が  $n$  に比べて非常に小さいならば（ $k \ll n$ ）、一般的なグループ鍵配送法よりも大幅な効率化が実現できる。例えば、1 0 0 0 0 台の加入者端末を持つシステム（ $n = 1 0 0 0 0$ ）で、排除対象端末を 1 0 0（ $k = 1 0 0$ ）とすると、一般的なグループ鍵配送法では 1 0 0 0 0  
15 回に比例した処理が必要だったのに対し、同公報に記載された従来技術 1 によれば 1 0 0 回に比例した処理で実現することが可能である。

しかし、加入者端末数が数百万台に上るようなシステム（例えば携帯電話などのモバイル端末を対象としたシステム）等では、  
20 グループの大きさにあわせて、排除対象端末の最大数  $k$  も大きく取る必要がある（例えば数千～数万）。このため、計算能力が低い端末などでは、復号処理に要する  $k$  に比例した計算負荷が無視できない。したがって、 $k$  に比例しない、可能ならば定数回の復  
25 号処理によりグループ鍵配送が望まれる。

この問題を解決すべくなされた従来技術として、特開 2 0 0 1 - 2 0 3 6 8 2 号公報がある（従来技術 2）。

同公報に開示された従来技術 2 は、加入者端末数  $n$ 、及び排除  
30 対象端末の最大数  $k$  に依存せず、2 回の冪剰余演算のみで復号処理を実現する。したがって、非常に多くの加入者端末を持つシステムにおいても、高速にグループ鍵の配送を完了することができ

る。

放送型暗号通信システムにおいて、プロトコル中のメンバーを次のように定義する。

5      鍵配布サーバ：セットアップ時に、システムパラメータを決定し、各加入者端末に対して個人鍵を配布する信頼機関。グループ鍵配送時には、どの加入者端末を排除するかを決定した上で、グループ鍵をブロードキャストにより配送する。鍵配布サーバを  $S$  と表す。

10      加入者端末：鍵配布サーバからのブロードキャストを受信する端末。加入者端末  $i$  は、セットアップ時に鍵配布サーバから個人鍵  $s_i$  を受け取る。加入者端末の集合を  $\Phi = \{1, \dots, n\}$  とする ( $n = |\Phi|$  は加入者端末の総数)。

15      排除された加入者端末：鍵配布サーバにより排除された加入者端末。1 回目のグループ鍵配送において排除される  $d$  ( $< k$ ) 個の加入者端末の集合を  $\Lambda_1$  ( $\subset \Phi$ ) とする。一度排除された加入者端末は、それ以降のラウンドでグループ鍵を復号することはいないため、複数のラウンドで重複して排除されることはない。すなわち、 $\Lambda_1 \cap \Lambda_{1'} = \{0\}$  ( $1 \neq 1'$ ) を満たす。また、排除された加入者端末の総数は、ラウンド全体を通じて  $k$  を超えないものとする (即ち、 $|\cup \Lambda_i| \leq k$ )。

20      有効な加入者端末：排除されていない加入者端末。1 回目のグループ鍵配送において有効な加入者端末の集合を  $\Omega_1$  ( $= \Phi \setminus \cup_{j=1}^1 \Lambda_j$ ) とする。

25

以上のように定義された放送型暗号システムでは、1 ラウンドにおいて、加入者端末全体  $\Phi$  のうち、有効な加入者端末  $\Omega_1$  に対して  $U_1$  が配送される。 $U_1$  を用いてメッセージを暗号化することで、グループ  $\Omega_1$  内における放送型暗号通信が可能になる。すなわち、

30

1.  $\Omega_0 = \Phi$  とする。鍵配布サーバは、各加入者  $i \in \Phi$  に対して、グループ鍵  $U_0$  及び個人鍵  $key_i$  を Point-to-Point の鍵配送プ

ロトコルで配送する。

2.  $l \geq 1$  に対して、以下の処理を繰り返す（この処理の1回の繰り返しを、以後「 $l$ ラウンド」と呼ぶ）。

(a) 鍵配布サーバが  $\Lambda_l \subset \Omega_{l-1}$  を決定する。

5 (b)  $k \geq \sum_{j=1}^l |\Lambda_j|$  であれば、 $\Phi := \Omega_{l-1}$ 、 $U_0 := U_{l-1}$  として1へ戻る。

(c) 鍵配布サーバが  $\Omega_l$  に対して  $U_l$  を計算するためのヘッダ  $H_l$  を配送する。

(d)  $v \in \Omega_l$  は、 $H_l$  及び  $key_v$  を用いて  $U_l$  を計算する。

10 (e) 鍵配布サーバ及び  $\Omega_l$  は、 $U_l$  を用いて放送型暗号通信を行う。

また、これ以降の説明では、次のパラメータを用いる。 $p$ 、 $q$  は  $q \mid p-1$  を満たす大きな素数であり、 $g$  は有限体  $Z_p$  上の位数  $q$  の元とする。 $p$ 、 $q$  のサイズは、 $g$  を生成元として構成される群  $GF(q)$  上での離散対数問題が計算量的に困難であるように設定するものとする。また、これ以降の説明において、特に記述のない場合、演算は、全て  $\text{mod } p$  上で行われるものとする。

20 なお、詳述はしないが、位数  $p$  の素体の上での構成法以外にも、離散対数問題が計算量的に困難となるような任意の群  $GF(q)$  上で定義することができる。例えば、(1) 位数  $p$  の素体上での乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応させることにより構成される群、(2) 素数  $p$  に代えて素数  $p'$  の冪乗数とし、素数  $p'$  を法とする剰余演算に代えて  $GF(p')$  の拡大体上での演算を行なうことにより構成される群、などがある。

30  $E(\text{key}, \text{message})$  は、鍵 ( $\text{key}$ ) を用いた対称鍵暗号によるメッセージ ( $\text{message}$ ) の暗号化を示す。 $n$  は加入者端末の総数、 $k (< n)$  は排除対象端末の最大数である。

以上の前提の下で、放送型暗号通信システムは、以下のような

安全性・効率上の4つの要件を満たすことが要求される。

1. 有効な加入者端末  $v \in \Omega_i$  は、単独でグループ鍵  $U_i$  を（多項式時間で）復号できる。
2. 排除された  $k$  個の加入者端末の持つ個人鍵を用いても、排除されたラウンド以降のグループ鍵を（確率的多項式時間で）復号することができない。
3. グループ鍵を配送するためのヘッダの長さや各加入者端末が持つ個人鍵のサイズが加入者端末の総数に依存しない。
4. グループ鍵を計算するためのヘッダを受け取ってから、グループ鍵の復号を完了するまで（復号処理）に要する冪剰余演算の回数が  $n$ 、 $k$  に依存しない。

上記要件1は、加入者端末が単独で効率的に復号できるための要件である。放送型暗号通信において、加入者端末が復号時に他の端末と通信する必要がないときには、ネットワークに対して余計なトラフィックを発生させないために重要である。

要件2は、排除された加入者端末が結託してもセッション鍵を復号できないために必要である。

要件3は、非常に多くの加入者端末を持つ場合に処理が大きくなること防ぐために必要である。

要件4は、大規模なグループにおいて  $k$  も大きく設定する必要がある場合に、 $n$  や  $k$  に依存しない処理量でグループ鍵を復号するための要件である。

いわゆる Spare Shadow Attack 及び  $r$  publish attack は、要件2に包含される。Secret Publish Attack は閾値型のプロトコルでは本質的に対応することはできない。ただし、秘密を公開してしまう攻撃者を  $w$  人としたとき、不正者の結託が  $k - w$  人以下であれば安全性が維持されることから、不正に加担する加入者端末が併せて  $k$  以下という条件でプロトコルの安全性を評価することで、要件2と同じ枠組みで安全性を議論することは可能である。

上述した従来技術 1 は、上記の要件 1、2、3 を満足する。配布される暗号文の長さが定数時間の  $O(k)$  であり、かつ個人鍵のサイズが  $O(1)$  であり、極めて効率が良い。しかし、グループ鍵の復号処理に要する冪剰余演算の回数は  $O(k)$  であり、またそれを事前計算に移行させることもできないため、要件 4 を満たさない。

従来技術 2 は、要件 4 の必要性に着目し、これを満足する手法を提示している。だが、以下に示す分析により、従来技術 2 は安全性上最も重要である要件 2 を満たしていない。すなわち、有限回グループ鍵を配送されると、排除されていない加入者端末はシステム全体の秘密情報を求めることが可能であり、それ以後の排除を無効にすることが可能である（例えば  $k \geq 5$  の場合、3 回のグループ鍵配送で攻撃可能である）。

以下に、従来技術 2 が要件 2 を満足しないことを示す。まず、従来技術 2 による放送型暗号通信の手法を説明する。

#### 1. セットアップ

鍵配布サーバは、排除対象端末の最大数  $k$  を設定し、次の数 1 式に示す  $Z_q$  上の  $k$  次多項式

数 1

$$F(x) = \sum_{j=0}^k a_j x^j$$

$$G(x) = \sum_{j=0}^k b_j x^j$$

をランダムに選択する。 $F(0) = S$ 、 $G(0) = T \pmod{q}$  は、鍵配布サーバだけが知る秘密鍵である。鍵配布サーバは、 $key_i = (s_i, f_i) = (F(i), g^{G(i)/F(i)})$  ( $i = 1, \dots, n$ ) を各加入者端末  $i$  に秘密通信路を用いて配布する。また、鍵配布サーバは、 $U_0 \in GF(q)$  をランダムに選択しブロードキャストする。

#### 2. グループ鍵暗号化

1 ( $\geq 1$ ) ラウンドにおけるグループ鍵  $U_1$  を次のように配送する。 $r_1 \in \mathbb{Z}_q$  をランダムに選び、 $X_1 = g^{r_1}$  を求める。次に  $d$  個の排除される加入者端末の集合  $\Lambda_1$  を決定する。 $k-d$  個の整数を  $n+k(R-1)$  と  $n+kR$  の間から選び、それらからなる集合を  $\Theta_1$  とする。鍵配布サーバは、 $M_{11}, \dots, M_{1k}$  を次の数 2 式にて求める。

数 2

$$M_{1j} = r_1 F(j) + G(j) \bmod q \quad (j \in \Lambda_1 \cup \Theta_1)$$

最後に、鍵配布サーバは、 $E(U_{1-1}, B_1) = E(U_{1-1}, X_1 || [ (j, M_{1j}) | j \in \Lambda_1 \cup \Theta_1 ] )$  を求め、ブロードキャストする。1 ラウンドに共有されるグループ鍵は  $U_1 = g^{r_1 s + T}$  である。

### 3. グループ鍵復号

1 ラウンドの有効な加入者端末  $v \in \Omega_1$  は、 $v \in \Omega_{1-1}$  であるから、 $U_{1-1}$  を 1-1 ラウンドで得ている。加入者端末  $v$  は、受信した暗号文  $E(U_{1-1}, B_1)$  について、 $U_{1-1}$  を用いて  $B_1$  を復号する。次に、 $B_1$  の情報を用いて、グループ鍵  $U_1$  を次の数 3 式にて計算する。

数 3

$$U_1 = (X_1 f_v)^{W_{11}} g^{W_{12}}$$

ここで、

数 4

$$\begin{aligned} W_{11} &= s_v L(v) \bmod q \\ W_{12} &= \sum_{j \in \Lambda_1 \cup \Theta_1} (M_{1j} L(j)) \bmod q \end{aligned}$$

また、 $L(j)$  は Lagrange の多項式補間係数で、

数 5

$$L(j) = \prod_{t \in \Lambda_1 \cup \Theta_1 \cup \{v\} \setminus \{j\}} t / (t - j) \bmod q$$

次に、上記従来技術 2 の手法が要件 2 を満たさないことを示す。  
 具体的に、R ラウンドの有効な任意の加入者端末  $\forall v \in \Omega_R$  が、鍵  
 配布サーバだけが知るべき秘密情報 S、T を導出する方法を示す。  
 v は 1 ~ R ラウンドにおいて  $(j, M_{ij})$  ( $i = 1, \dots, R$ ,  
 5  $j = 1, \dots, k$ ) を得るが、これは次の数 6 式の関係を満た  
 す。

数 6

$$M_{ij} = r_i \sum_{t=0}^k a_t j^t + \sum_{t=0}^k b_t j^t \bmod q \quad (i=1, \dots, R, j \in \Lambda_i \cup \Theta_i, |\Lambda_i \cup \Theta_i|=k)$$

ここで、j は既知であるため、 $2k + 2 + R$  個の変数  $a_0, \dots,$   
 10  $a_k, b_0, \dots, b_k, r_1, \dots, r_R$  に対し、 $kR$  個の方程式  
 を得ることができる。つまり、R が次の数 7 式を満たす場合、鍵  
 配布サーバが持つ全ての秘密鍵 S ( $= a_0$ ), T ( $= b_{10}$ ) を導出  
 することができてしまう。

数 7

$$2k + 2 + R \leq kR \quad \Leftrightarrow \quad R \geq \frac{2(k+1)}{k-1}$$

例えば、 $k \geq 5$  であれば、3 ラウンドには全ての有効な加入者  
 端末が鍵配布サーバの秘密鍵 (S や T など) を求められる。これ  
 により、従来技術 2 が要件 2 を満たしていないことがわかる。

20 そこで本発明は、上述した 4 つの要件を全て満足し、安全性が  
 高く高速なグループ鍵の更新方法を提供することを目的とする。

また本発明は、上記の目的に加えて、安全性が高く効率の良い  
 放送型暗号通信を実現することを目的とする。

25 発明の開示

上記の目的を達成する本発明は、暗号化された情報を復号する  
 ための鍵を配布する鍵配布サーバと、当該情報を使用する所定台  
 数の加入者端末とを備えた暗号通信システムとして実現される。  
 この鍵配布サーバは、情報の復号に用いる暗号化された第 1 のグ  
 30 ループ鍵と、この第 1 のグループ鍵の復号処理を実行するための

加入者端末ごとに個別の復号情報と、グループ鍵の更新後に更新された第2のグループ鍵の復号処理の一部を実行するための加入者端末ごとに個別の鍵更新情報とを加入者端末に配布し、この加入者端末は、予め取得した第1のグループ鍵を復号するための  
5 鍵更新情報に基づく処理結果と鍵配布サーバから配布された復号情報とを用いて鍵配布サーバから配布された第1のグループ鍵を復号することを特徴とする。グループ鍵の復号処理を時間的に分散することにより、グループ鍵更新時の処理を軽減している。

10 ここで、加入者端末は、鍵更新情報を用いたグループ鍵の復号処理の一部を、このグループ鍵の配布前に実行する。グループ鍵を復号する処理の一部を加入者端末において事前に行っておくことにより、グループ鍵の更新において、安全性を損なうことなく、新しいグループ鍵が配布された後の処理に要する時間の短縮  
15 を実現している。

また好ましくは、鍵配布サーバは、第1のグループ鍵を復号するための鍵更新情報を、この第1のグループ鍵に更新される前の第3のグループ鍵と共に加入者端末に配布する。

さらに、鍵配布サーバは、グループ鍵を更新した場合に、加入  
20 者端末のうち排除対象端末を設定し、この排除対象端末以外の加入者端末が更新されたグループ鍵を復号可能となる復号情報を、更新されたグループ鍵と共に加入者端末に配布する。

また、上記の目的を達成する他の本発明は、暗号化された情報を復号するための鍵を配布する次のように構成された鍵配布サ  
25 ーバとして実現される。この鍵配布サーバは、情報の復号に用いる第1のグループ鍵を生成し暗号化する手段と、この第1のグループ鍵の復号処理を実行するための加入者端末ごとに個別の復号情報を生成する手段と、グループ鍵の更新後に更新された第2  
30 のグループ鍵の復号処理の一部を実行するための加入者端末ごとに個別の鍵更新情報を生成する手段と、第1のグループ鍵と復号情報と鍵更新情報とを加入者端末に配布する手段とを備える

ことを特徴とする。

また、上記の目的を達成するさらに他の本発明は、次のように構成された端末装置としても実現される。この端末装置は、暗号化された情報を復号するための暗号化されたグループ鍵とこのグループ鍵を復号するための復号情報とを所定の鍵配布サーバから取得する手段と、グループ鍵の復号処理の一部をこのグループ鍵の配布前に実行する手段と、このグループ鍵の復号処理の一部に基づく処理結果と鍵配布サーバから取得した復号情報とを用いてグループ鍵を復号する手段とを備えることを特徴とする。

さらに本発明は、コンピュータを制御して上記の鍵配布サーバや端末装置として機能させるプログラムとしても実現される。このプログラムは、磁気ディスクや光ディスク、半導体メモリその他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供することができる。

また、本発明は、暗号化された情報を復号するための鍵を、この情報を使用する所定台数の端末で共有する、次のような鍵共有方法として実現される。すなわち、この鍵共有方法は、情報の復号に用いる暗号化されたグループ鍵を復号するための復号処理の一部が、このグループ鍵の配布前に、端末において実行されるステップと、グループ鍵とこのグループ鍵の復号処理の残りの一部を実行するための端末ごとに個別の復号情報とが、端末に配布されるステップと、配布された復号情報と事前に実行された復号処理の一部の結果とを用いたグループ鍵の復号処理が、端末において実行されるステップとを含むことを特徴とする。

#### 図面の簡単な説明

図 1 は本実施の形態による放送型暗号通信システムの概略構成を説明する図である。

図 2 は本実施の形態による暗号通信の処理の流れを説明する

フローチャートである。

図 3 は本実施の形態を適用したピア・ツー・ピア型ネットワークシステムの構成を示す図である。

5 図 4 は本実施の形態を適用したリアルタイムコンテンツ配信システムの構成を示す図である。

図 5 は本実施の形態を適用した携帯電話を対象とするサービス提供システムの構成を示す図である。

図 6 は本実施の形態を適用したマルチメディアコンテンツ配信システムの構成を示す図である。

10 図 7 は本実施の形態を適用した秘密放送システムの構成を示す図である。

発明を実施するための最良の態様

以下、添付図面に示す実施の形態に基づいて、この発明を詳細  
15 に説明する。

図 1 は、本実施の形態による放送型暗号通信システムの概略構成を説明する図である。

図 1 を参照すると、本実施の形態による放送型暗号通信システムは、暗号通信に用いられるグループ鍵を生成し配布する鍵配布  
20 サーバ 10 と、鍵配布サーバ 10 から配布されたグループ鍵を取得しこれを用いて暗号通信を行う加入者端末 20 とを備える。

鍵配布サーバ 10 は、ワークステーションやパーソナルコンピュータ、その他のネットワーク機能を備えたコンピュータ装置にて実現され、セットアップ時に、システムパラメータを決定し、  
25 各加入者端末 20 に対して個人鍵を配布する。グループ鍵配送時には、どの加入者端末 20 を排除するかを決定した上で、グループ鍵を暗号化し、ブロードキャストにより配送する。個人鍵やグループ鍵の生成、配送等の処理は、例えばプログラム制御された  
30 CPU の機能として実現される。

加入者端末 20 は、ワークステーションやパーソナルコンピュータ、携帯電話、PDA (Personal Digital Assistant)、その

他のネットワーク機能を備えた情報端末機器にて実現され、鍵配布サーバ10からのブロードキャストを受信する。加入者端末*i*（*i*番目の加入者端末20）は、セットアップ時に鍵配布サーバ10から個人鍵*s<sub>i</sub>*を受け取る。そして、この個人鍵*s<sub>i</sub>*を用いて暗号化されているグループ鍵を復号し、さらにこのグループ鍵を用いて所定のメッセージを復号して使用する。これらの処理は、例えば、プログラム制御されたプロセッサにて実現される。加入者端末20の集合を  $\Phi = \{1, \dots, n\}$  とする（ $n = |\Phi|$  は加入者端末20の総数）。

加入者端末20は、全体で、鍵配布サーバ10から配布されたグループ鍵を用いて暗号通信を行うグループ  $\Phi$  を構成する。このグループを構成する個々の加入者端末20は、初期的には全て暗号通信に参加できる「有効な加入者端末」であるが、何らかの理由により「排除された加入者端末」となった後は、暗号通信には参加できない。すなわち、個人鍵を用いてグループ鍵を復元することができない。

本実施の形態における通信形態は、鍵配布サーバ10あるいは所定のサーバと加入者端末20との間で情報がやりとりされるクライアント／サーバ型のシステムであっても良いし、加入者端末20相互間で情報をやりとりするピア・ツー・ピア（Peer to Peer）型のシステムであっても良い。すなわち、加入者端末20で使用されるメッセージ（コンテンツ）の提供者は、鍵配布サーバ10とは別個に存在しても良い。

放送型暗号通信システムにおけるグループ鍵を用いた暗号通信は、グループ鍵のセットアップ、グループ鍵を用いた情報の暗号化、グループ鍵を用いた情報の復号、及び鍵更新の4つのフェーズを含む。

図2は、本実施の形態による暗号通信の処理の流れを説明するフローチャートである。

本実施の形態では、暗号化されたグループ鍵の復号処理の中で

排除対象端末の最大数  $k$  に依存する計算部分を事前計算（鍵更新処理）に切り分ける。これにより、証明可能な安全性を保ちつつ、鍵更新処理を除く部分のグループ鍵の復号処理を2回の冪剰余演算で高速に実行可能としている。以下、本実施の形態による暗号通信におけるプロトコルの構成法を説明する。なお、以下の説明において、受信者とは、加入者端末20のユーザであり、加入者自身である。

### 1. セットアップ

10  $Z_q$  上のランダムな  $k$  次一変数多項式  
数8

$$F(x) = S + \sum_{j=1}^k a_j x^j$$

$$G_1(x) = T_1 + \sum_{j=1}^k b_{1j} x^j$$

15 を選択する。  $F(0) = S$ 、  $G_1(0) = T_1$  を鍵配布サーバ10の秘密鍵とする。鍵配布サーバ10は、  $key_1 = (s_1, f_1) = (F(i), g^{G_1(i)/F(i)})$  を第1ラウンドの受信者  $i$  の復号鍵として、各加入者端末  $i \in \{1, \dots, n\}$  に秘密に配布する。グループ鍵  $U_0 \in GF(q)$  は、全ての加入者端末20に対して配布される（ステップ201）。

20

### 2. 1ラウンドにおけるグループ鍵暗号化

鍵配布サーバ10は、  $r_1 \in Z_q$  をランダムに選択し、  $X_1 := g^{r_1}$  を求める。次に、  $d$  個の排除される加入者端末20の集合  $\Lambda_1$  を決定する（ステップ202）。  $k-d$  個の整数を  $n+k(R-1)$  と  $n+kR$  の間から選び、それらからなる集合を  $\Theta_1$  とする。鍵配布サーバ10は  $M_{11}, \dots, M_{1k}$  を次の数9式にて求める。  
数9

$$M_{1j} = r_1 F(j) + G_1(j) \bmod q \quad (j \in \Lambda_1 \cup \Theta_1)$$

また、有効な加入者端末20である  $\Omega_1$ （以下、加入者端末  $\Omega_1$ ）

が 1 ラウンドの配送鍵  $U_1$  を計算するために必要なヘッダ情報  $H_1$  を、次の数 10 式にて計算する (ステップ 203)。

数 10

$$B_1 = \langle X_1 \parallel \{(j, M_{1j}) \mid j \in \Lambda_1 \cup \Theta_1\} \rangle$$

$$H_1 = E(U_{1-1}, B_1)$$

- 5      ここで、1 ラウンドにおいて有効な加入者端末  $\Omega_1$  にて共有されるグループ鍵は、 $U_1 = g^{rs+T_1}$  である。

次に、1+1 ラウンドにグループ鍵を配送するための (すなわち、加入者端末 20 が 1+1 ラウンドのグループ鍵の復号処理における鍵更新処理で用いる) 鍵更新情報を生成する。鍵配布サーバ

- 10    バ 10 は、 $b_{1+1,j} \in Z_q (j = 0, \dots, k)$  をランダムに選択し、  
 $(u_{10}, \dots, u_{1k}) = (g^{b_{1+1,0}}, \dots, g^{b_{1+1,k}})$  を求め、次の数 11 式により 1 ラウンドのグループ鍵  $U_1$  で暗号化して  $C_1$  を求める (ステップ 204)。

数 11

15      
$$C_1 = E(U_1, u_{10} \parallel \dots \parallel u_{1k})$$

そして、鍵配布サーバ 10 は、 $(H_1, C_1)$  を全ての加入者端末 20 (すなわち  $\Phi$ ) に対してブロードキャストで配布する (ステップ 205)。

### 20    3. 1 ラウンドにおけるグループ鍵復号

1 ラウンドにおける復号可能な加入者端末 20 である加入者端末  $v$  ( $\in \Omega_1$ ) は、次の数 12 式により、1 ラウンドの復号を行う (ステップ 206)。

数 12

$$U = (X_1 f_{1v})^{W_{11}} g^{W_{12}}$$

$$W_{11} = s_v L(v) \bmod q$$

$$W_{12} = \sum_{j \in \Lambda \cup \Theta} M_{1j} L(j) \bmod q$$

ここで、

25      
$$L(j) = \prod_{t \in \Lambda \cup \Theta \cup \{v\} \setminus \{j\}} t / (t - j) \bmod q$$

すなわち、ここでは 1-1 ラウンドで配布された情報に基づい

て事前計算された  $f_{i,v}$  と、ステップ 205 で配布された  $H_i$  から  
 解読される  $B_i$  とを用いて  $i$  ラウンドのグループ鍵  $U_i$  を復号し  
 ている。

5 4.  $i+1$  ラウンドへ向けての鍵更新処理（事前計算）

有効な各加入者端末  $v \in \Omega_i$  は、鍵配布サーバ 10 から配布さ  
 れた  $C_i$  に含まれる鍵更新情報を用い、次の数 13 式にて事前計  
 算（すなわち  $i+1$  ラウンドのグループ鍵の配布前の処理）であ  
 る鍵更新処理を行う（ステップ 207）。

10 数 13

$$f_{i+1,v} = \left( \prod_{j=0}^k u_{ij}^{v_j} \right)^{1/s_v}$$

また、鍵配布サーバ 10 は、 $i+1$  ラウンドのグループ鍵の生  
 成に先立って、次の数 14 式の事前計算を実行する。

数 14

$$T_{i+1} = b_{i+1,0} \bmod q$$

$$G_{i+1}(x) = \sum_{j=0}^k b_{i+1,j} x^j \bmod q$$

15

これら加入者端末 20 及び鍵配布サーバ 10 による鍵更新処  
 理（事前計算）は、 $i$  ラウンドのグループ鍵と共に配布された情  
 報を用いて、 $i+1$  ラウンドのグループ鍵が配布される前までに  
 20 実行しておく。

以上のように構成される本実施の形態による放送型暗号通信  
 システムが、上述した安全性・効率上の 4 つの要件を満たすかど  
 うかを検討する。

25 まず、本実施の形態は、加入者端末 20 間の通信を必要として  
 いないことから、要件 1 を満たすことは明らかである。

また、本実施の形態において配布される暗号文の長さは  $O(k)$ 、

個人鍵のサイズは $O(1)$ であり、要件3も満たす。

さらに、本実施の形態における復号処理は2回の冪剰余演算で構成されており、要件4も満たしている。

5 次に、本実施の形態が残る要件2を満たすことを示す。

まず、要件2で述べられている「排除された $k$ 個の加入者端末の持つ個人鍵を用いる」攻撃者をモデル化する。この攻撃者は、 $R$ ラウンドまでに排除されたメンバ $k$ 人の復号鍵、及び $R$ ラウンド以前に受け取った情報から $R$ ラウンドのグループ鍵を多項式

10 時間で求めるアルゴリズム $M_1$ としてモデル化できる。一般性を失わずに( $k$ 個の)排除された加入者端末20を $i = 1, \dots, k$ とする。 $M_1$ のインプットは、

$\langle g, p, q, k, U_0, (s_1, \dots, s_k), (f_{11}, \dots, f_{1k}), (H_1, C_1), \dots, (H_R, C_R) \rangle$

15 である。

このようにモデル化すると、要件2は、DDH問題 (Decision Diffie-Hellman Problem) を用いて次のように言い換えることができる。

20 (命題)

「DDH問題を解く多項式時間アルゴリズムが存在しない限り、 $M_1$ は存在しない」

DDH問題とは、 $g, h \in GF(q)$ ,  $a, b \in \mathbb{Z}_q$ をランダムに選んだとき、 $GF(q)$ 上において、 $D = \langle g, h, g^a, h^a \rangle$

25 (この形を「Diffie-Hellmanの組」と呼ぶ)と $R = \langle g, h, g^a, h^a \rangle$ とを有意な確率を持って区別する判定問題である。DDH問題を多項式時間で解くアルゴリズムは知られていない。すなわち、計算量的に困難であると仮定できる数学的な問題であり、上記の命題から $M_1$ は存在しない。したがって、本実施の形態は

30 要件2を満足する。

以上のように、本実施の形態による放送型暗号通信システムの

グループ鍵共有方法によれば、グループ鍵を更新するにあたって、証明可能な安全性を確保でき、かつグループ鍵の復号処理の一部を事前計算にて当該グループ鍵が配布される前に行うことにより、更新されたグループ鍵が配布された後の処理では加入者端末数  $n$ 、及び排除対象端末の最大数  $k$  に依存せず、2 回の冪剰余演算のみで復号処理を実現できる。したがって、加入者端末 20 の数が膨大であるネットワークシステムにおいて、特に有効である。

次に、本実施の形態による放送型暗号通信システムを種々のネットワークシステムに適用した場合の構成例を説明する。

10

〔ピア・ツー・ピアにおけるグループメンバー管理〕

ピア・ツー・ピア (Peer to Peer: P2P) 型のネットワークシステムにおいて、グループ内通信を安全かつ高速に行うために、本実施の形態を用いることができる。すなわち、ネットワークシステムにおけるグループ内の全てのピア (Peer) が 1 つの鍵 (グループ鍵) を共有し、放送型暗号通信を行う。

図 3 は、本実施の形態を適用したピア・ツー・ピア型ネットワークシステムの構成を示す図である。図 3 において、対象であるネットワークシステムのグループマネージャーが本実施の形態の鍵配布サーバ 10 を構成し、グループ内の各ピア (Peer) が加入者端末 20 を構成する。

このようなネットワークシステムでは、例えば jxta における leave などによって所定のピア (Peer) がグループから離脱した場合、それ以降のグループ内通信を安全に行うためには、新たなグループ鍵を残りのピア (Peer) の間で迅速に再共有する必要がある。一方で、ピア・ツー・ピア型ネットワークでは様々な端末がピア (Peer) となり得るため、非常に計算能力の限られた端末であっても容易にグループ鍵を入手できなければならない。本実施の形態は、このようなピア・ツー・ピア型ネットワークシステムにおけるグループメンバー管理に容易に適用できる。

30

本実施の形態を適用することにより、グループ鍵の復号処理は、2 回の冪剰余乗算で完了するため、大きな計算能力を必要としな

い。また、大規模なネットワークで適用した場合でも効率性を損なわずに高速にグループ鍵の更新を行い利用可能とすることができる。

5     〔リアルタイムコンテンツ配信システム〕

ゲーム機の高機能化に伴い、ゲーム機をピア（Peer）と見立ててピア・ツー・ピア型ネットワークを構成することにより、ユーザ間のインタラクションを容易にするようなオンラインゲームが出現している。すなわち、グループマネージャに相当するサーバがゲームコンテンツを各ゲーム機に提供し、各ゲーム機間でピア・ツー・ピア型の通信を行いながらゲームを進行する。

図4は、本実施の形態を適用したこの種のコンテンツ配信システムの構成を示す図である。図4において、ゲームコンテンツを配信するサーバが本実施の形態の鍵配布サーバ10を構成し、各ゲーム機が加入者端末20を構成する。

このような環境においては、グループ内での放送型暗号通信が頻繁に必要なことが予想されるが、その一方でグループからのメンバの離脱も頻繁に起こりえると考えられる。例えば、利用料金を滞納したユーザはグループへの接続を解除する必要がある。したがって、グループからメンバが離脱する際に要する、グループ鍵共有のための復号処理時間を短縮することは、アプリケーションの利用性を高める。

本実施の形態による放送型暗号通信は、高速な復号処理を実現し、大規模なネットワークに対応可能であるため、図4に示すシステムにおけるコンテンツの配信に適用することができる。すなわち、グループ鍵を高速に共有することができ、これにより暗号化されたコンテンツを受信と同時にリアルタイムで復号することが可能になる。また、時間を要する鍵更新処理は、コンテンツ受信後に当該コンテンツ実行時の余剰処理能力を用いて行うことができる。なお、ここではオンラインゲームを実行するためのコンテンツ配信を例として説明したが、ゲームの他にもリアルタイムで実行するような種々のコンテンツを配信する場合に、本実

施の形態による放送型暗号通信を適用できることは言うまでもない。

〔携帯電話加入者へのデータ配信〕

5 近年、携帯電話の利用は人口の過半数をカバーするほどに拡大している。そこで、数百万の携帯電話加入者に対してグループ暗号化通信のサービスを行う場面を考える。例えば、グループを構成した端末に対して特定のサービスを提供する場合などがある。

10 図5は、本実施の形態を適用した携帯電話を対象とするサービス提供システムの構成を示す図である。図5において、サービスを提供するサーバが鍵配布サーバ10を構成し、サービスの利用登録がなされている携帯電話が加入者端末20を構成する。

15 このようなネットワークシステムでは、サービスの利用料金を滞納したり、端末の紛失や盗難があった場合に、特定の端末の持つグループへのアクセス権限を無効化する必要がある。本実施の形態は、本発明を適用することで、非力な携帯電話に対しても利用可能な放送型暗号通信を実現できる。

〔マルチメディアコンテンツ配信システム〕

20 近年、DVDを用いたマルチメディアコンテンツ配信システムが爆発的に普及している。

図6は、本実施の形態を適用したマルチメディアコンテンツ配信システムの構成を示す図である。図6において、マルチメディアコンテンツを提供するコンテンツプロバイダが本実施の形態  
25 の鍵配布サーバ10を構成し、当該マルチメディアコンテンツの再生機が加入者端末20を構成する。

このシステムにおいて、DVDメディアは暗号化されたデジタルコンテンツ（映画や音楽、ソフトウェアなど）が記憶された状態で配布される。暗号化されたコンテンツは再生機に搭載された  
30 再生復号器内に保管される復号鍵を用いて復号される。復号鍵は再生復号器のメーカーごとに異なり、再生復号器の安全なメモリエリアに格納されている。だが、クラッカーの解析やメーカーの

不手際により、復号鍵が漏洩してしまう場面が起こり得る。この場合に、一部の復号鍵を使用不可能にする暗号化手法が必要となる。

5 本実施の形態を適用することにより、証明可能な安全性を確保して、一部の復号鍵を使用不可能にするための復号鍵の更新を行うことが可能となる。

#### 〔警察無線機の紛失・盗難に対応する秘密放送システム〕

10 警察無線は、グループ内秘匿通信の代表例である。警察官の所持する無線機以外の無線受信機を用いても通信が傍受できないようにすることが必要となる。

図7は、本実施の形態を適用した秘密放送システムの構成を示す図である。図7において、秘密放送の放送局が鍵配布サーバ10を構成し、各無線受信機が加入者端末20を構成する。

15 上記のように、警察無線のような秘密放送では、警察官の所持する無線機以外の無線受信機では通信を傍受できないような工夫が必要であるが、警察官が無線機を紛失したり盗難されたりした場合、本実施の形態により、かかる無線機を加入者端末20のグループ(Φ)から排除して新しいグループ鍵を共有することにより、紛失した無線機を利用不可能にすることができる。

#### 発明の効果

以上説明したように、本発明によれば、安全性が高く高速なグループ鍵の更新方法を提供することができる。

25 また本発明によれば、安全性が高く効率の良い放送型暗号通信を実現することができる。

## 請求の範囲

1. 暗号化された情報を復号するための鍵を配布する鍵配布サーバと、当該情報を使用する所定台数の加入者端末とを備えた暗号通信システムにおいて、

前記鍵配布サーバは、前記情報の復号に用いる暗号化された第1のグループ鍵と、当該第1のグループ鍵の復号処理を実行するための前記加入者端末ごとに個別の復号情報と、グループ鍵の更新後に更新された第2のグループ鍵の復号処理の一部を実行するための前記加入者端末ごとに個別の鍵更新情報とを前記加入者端末に配布し、

前記加入者端末は、予め取得した前記第1のグループ鍵を復号するための前記鍵更新情報に基づく処理結果と前記鍵配布サーバから配布された前記復号情報とを用いて前記鍵配布サーバから配布された前記第1のグループ鍵を復号することを特徴とする暗号通信システム。

2. 前記加入者端末は、前記鍵更新情報を用いた前記グループ鍵の復号処理の一部を、当該グループ鍵の配布前に実行することを特徴とする請求項1に記載の暗号通信システム。

3. 前記鍵配布サーバは、前記第1のグループ鍵を復号するための鍵更新情報を、当該第1のグループ鍵に更新される前の第3のグループ鍵と共に前記加入者端末に配布することを特徴とする請求項1に記載の暗号通信システム。

4. 前記鍵配布サーバは、前記グループ鍵を更新した場合に、前記加入者端末のうち排除対象端末を設定し、当該排除対象端末以外の加入者端末が更新された当該グループ鍵を復号可能な前記復号情報を、更新された当該グループ鍵と共に前記加入者端末に配布することを特徴とする請求項1に記載の暗号通信システム。

5. 暗号化された情報を復号するための鍵を配布する鍵配布サーバにおいて、

前記情報の復号に用いる第1のグループ鍵を生成し暗号化する手段と、

前記第1のグループ鍵の復号処理を実行するための加入者端末ごとに個別の復号情報を生成する手段と、

- 5      グループ鍵の更新後に更新された第2のグループ鍵の復号処理の一部を実行するための前記加入者端末ごとに個別の鍵更新情報を生成する手段と、

前記第1のグループ鍵と前記復号情報と前記鍵更新情報とを前記加入者端末に配布する手段と

- 10      を備えることを特徴とする鍵配布サーバ。

6.      前記復号情報を生成する手段は、前記加入者端末のうち排除対象端末を設定し、当該排除対象端末以外の加入者端末が当該グループ鍵を復号可能な前記復号情報を生成することを特徴とする請求項5に記載の鍵配布サーバ。

- 15      7.      暗号化された情報を復号するための暗号化されたグループ鍵と当該グループ鍵を復号するための復号情報とを所定の鍵配布サーバから取得する手段と、

前記グループ鍵の復号処理の一部を当該グループ鍵の配布前に実行する手段と、

- 20      前記グループ鍵の復号処理の一部に基づく処理結果と前記鍵配布サーバから取得した前記復号情報とを用いて前記グループ鍵を復号する手段と

を備えることを特徴とする端末装置。

- 25      8.      コンピュータを制御して、暗号化された情報を復号するための鍵を配布するプログラムであって、

前記情報の復号に用いる第1のグループ鍵を生成し暗号化する機能と、

前記第1のグループ鍵の復号処理を実行するための加入者端末ごとに個別の復号情報を生成する機能と、

- 30      グループ鍵の更新後に更新された第2のグループ鍵の復号処理の一部を実行するための前記加入者端末ごとに個別の鍵更新情報を生成する機能と、

所定の通信手段を介して前記第 1 のグループ鍵と前記復号情報と前記鍵更新情報とを前記加入者端末に配布する機能と

を前記コンピュータに実現させることを特徴とするプログラム。

- 5 9. 前記復号情報を生成する機能は、前記加入者端末のうち排除対象端末を設定し、当該排除対象端末以外の加入者端末が当該グループ鍵を復号可能な前記復号情報を生成することを特徴とする請求項 8 に記載のプログラム。

- 10 10. コンピュータを制御して、所定の機能を実現するプログラムであって、

所定の通信手段を介して、暗号化された情報を復号するための暗号化されたグループ鍵と当該グループ鍵を復号するための復号情報とを所定の鍵配布サーバから取得する機能と、

- 15 前記グループ鍵の復号処理の一部を当該グループ鍵の配布前に実行する機能と、

前記グループ鍵の復号処理の一部に基づく処理結果と前記鍵配布サーバから取得した前記復号情報とを用いて前記グループ鍵を復号する機能と

- 20 を前記コンピュータに実現させることを特徴とするプログラム。

11. コンピュータを制御して暗号化された情報を復号するための鍵を配布するプログラムを、当該コンピュータが読み取り可能に記録した記録媒体であって、

前記プログラムは、

- 25 前記情報の復号に用いる第 1 のグループ鍵を生成し暗号化する機能と、

前記第 1 のグループ鍵の復号処理を実行するための加入者端末ごとに個別の復号情報を生成する機能と、

- 30 グループ鍵の更新後に更新された第 2 のグループ鍵の復号処理の一部を実行するための前記加入者端末ごとに個別の鍵更新情報を生成する機能と、

所定の通信手段を介して前記第 1 のグループ鍵と前記復号情

報と前記鍵更新情報とを前記加入者端末に配布する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

12. コンピュータを制御して所定の機能を実現するプログラムを、当該コンピュータが読み取り可能に記録した記録媒体であって、

前記プログラムは、

所定の通信手段を介して、暗号化された情報を復号するための暗号化されたグループ鍵と当該グループ鍵を復号するための復号情報とを所定の鍵配布サーバから取得する機能と、

前記グループ鍵の復号処理の一部を当該グループ鍵の配布前に実行する機能と、

前記グループ鍵の復号処理の一部に基づく処理結果と前記鍵配布サーバから取得した前記復号情報とを用いて前記グループ鍵を復号する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

13. 暗号化された情報を復号するための鍵を、当該情報を使用する所定台数の端末で共有する鍵共有方法において、

前記情報の復号に用いる暗号化されたグループ鍵を復号するための復号処理の一部が、当該グループ鍵の配布前に、前記端末において実行されるステップと、

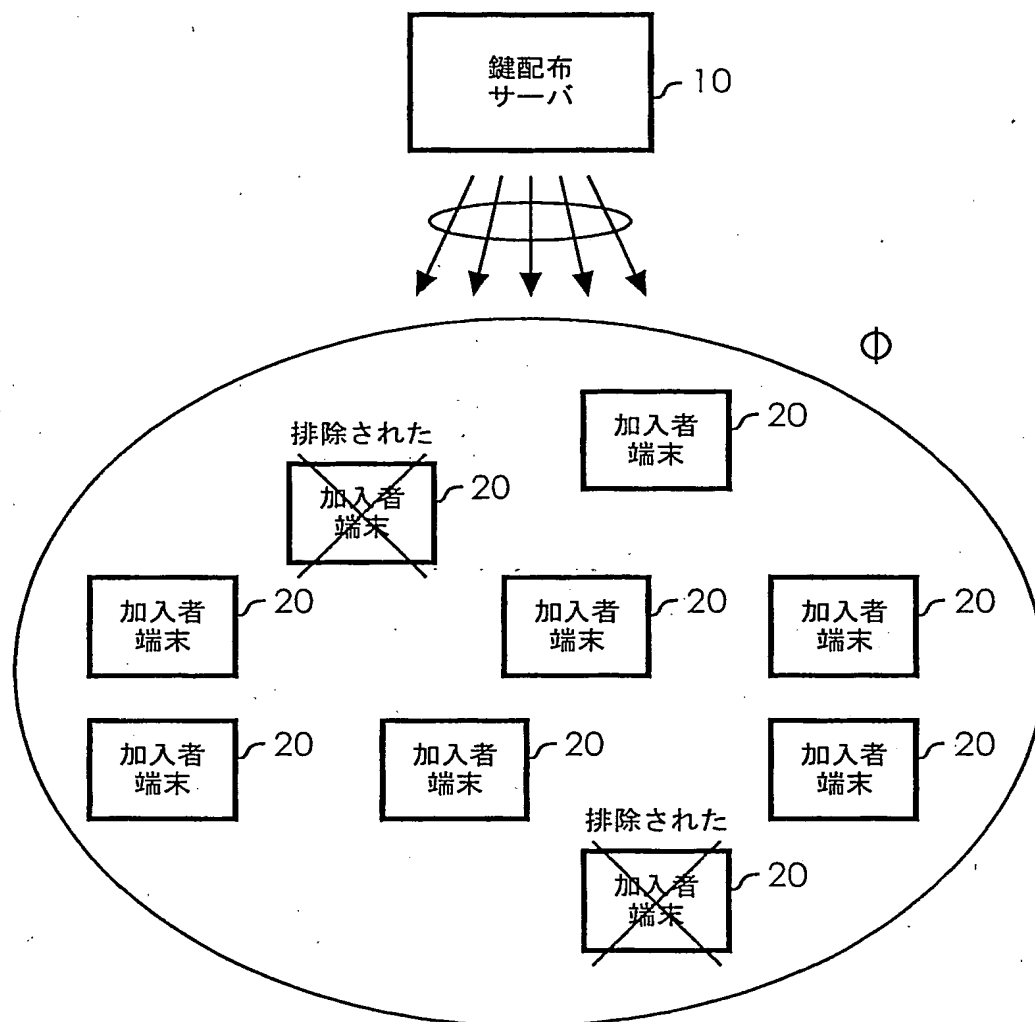
前記グループ鍵と、当該グループ鍵の復号処理の残りの一部を実行するための前記端末ごとに個別の復号情報とが、当該端末に配布されるステップと、

配布された前記復号情報と事前に実行された前記復号処理の一部の結果とを用いた前記グループ鍵の復号処理が、前記端末において実行されるステップと

を含むことを特徴とする鍵共有方法。

14. 前記グループ鍵の配布前に前記復号処理の一部を実行するための情報が、更新前の前記グループ鍵と共に前記端末に配布されることを特徴とする請求項13に記載の鍵共有方法。

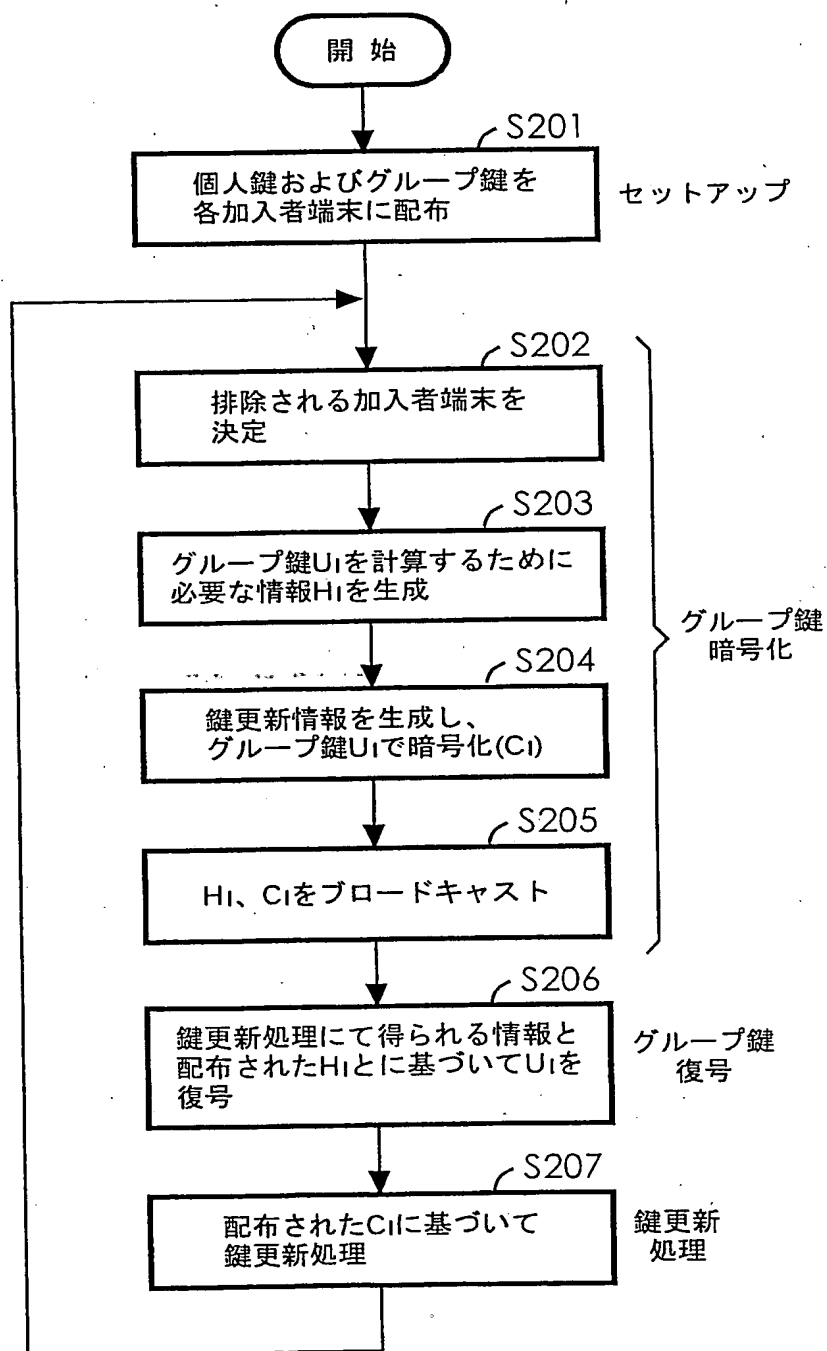
1/6



第 1 図

**THIS PAGE BLANK (USPTO)**

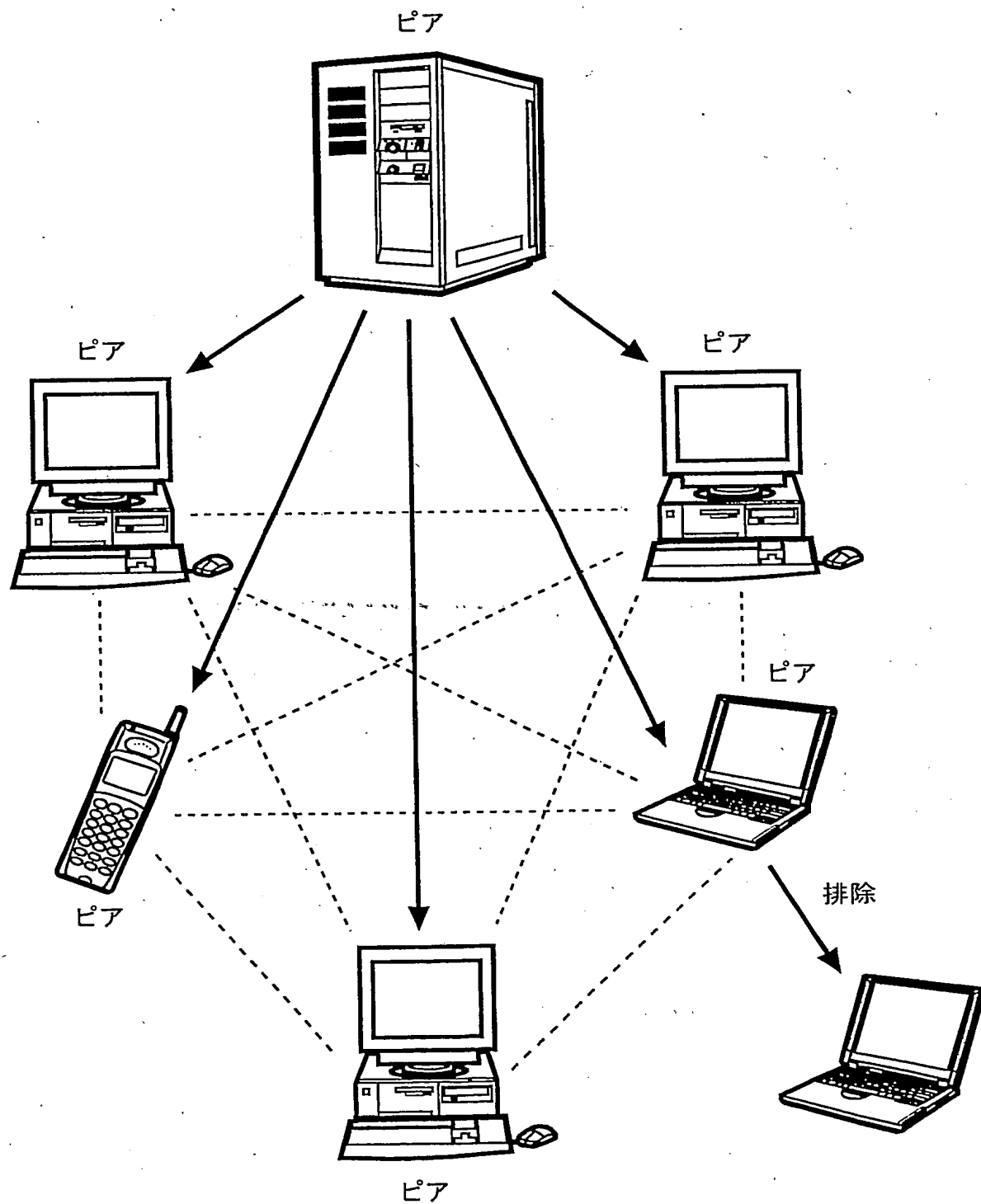
2/6



第 2 図

**THIS PAGE BLANK (USPTO)**

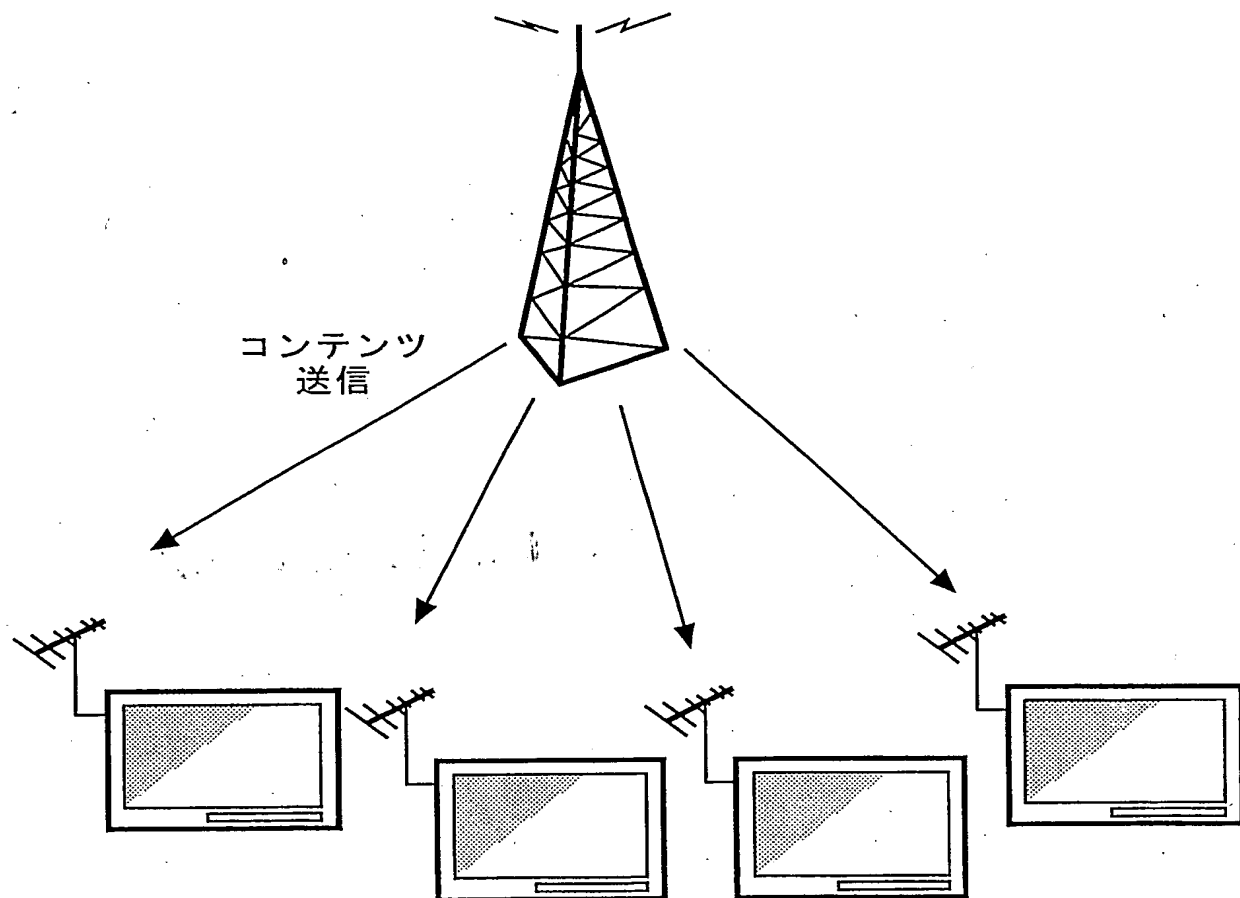
3/6



第 3 図

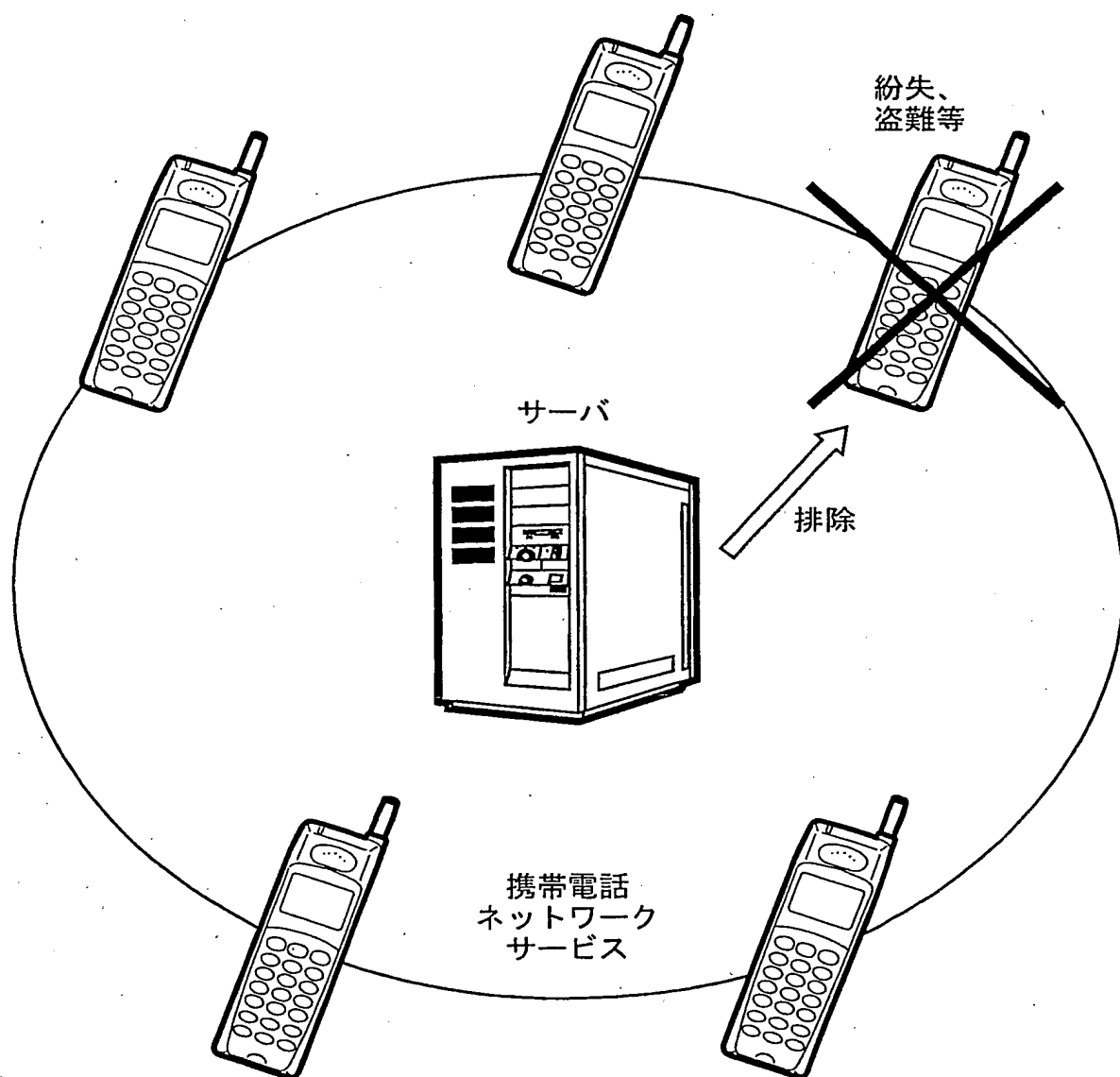
**THIS PAGE BLANK (USPTO)**

4/6



第 4 図

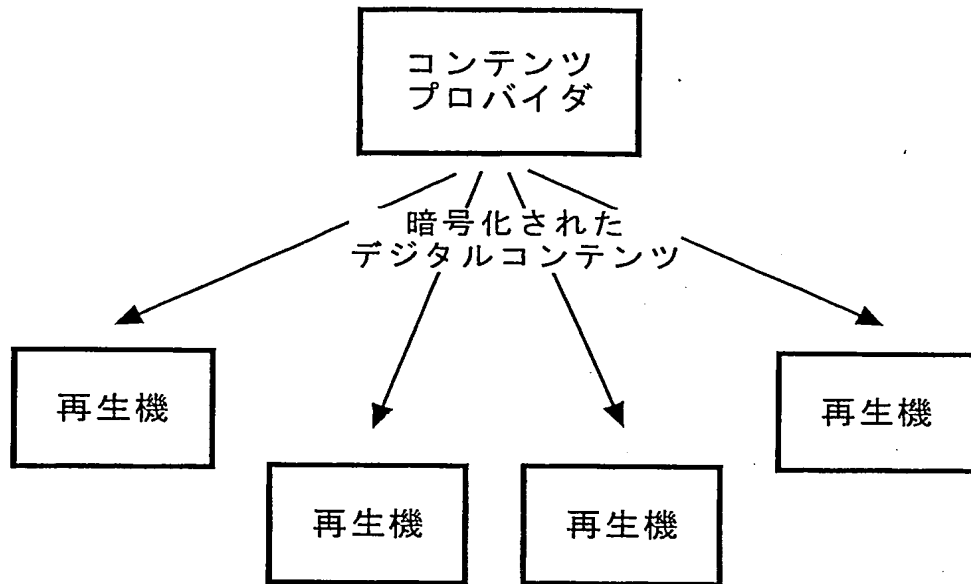
**THIS PAGE BLANK (USPTO)**



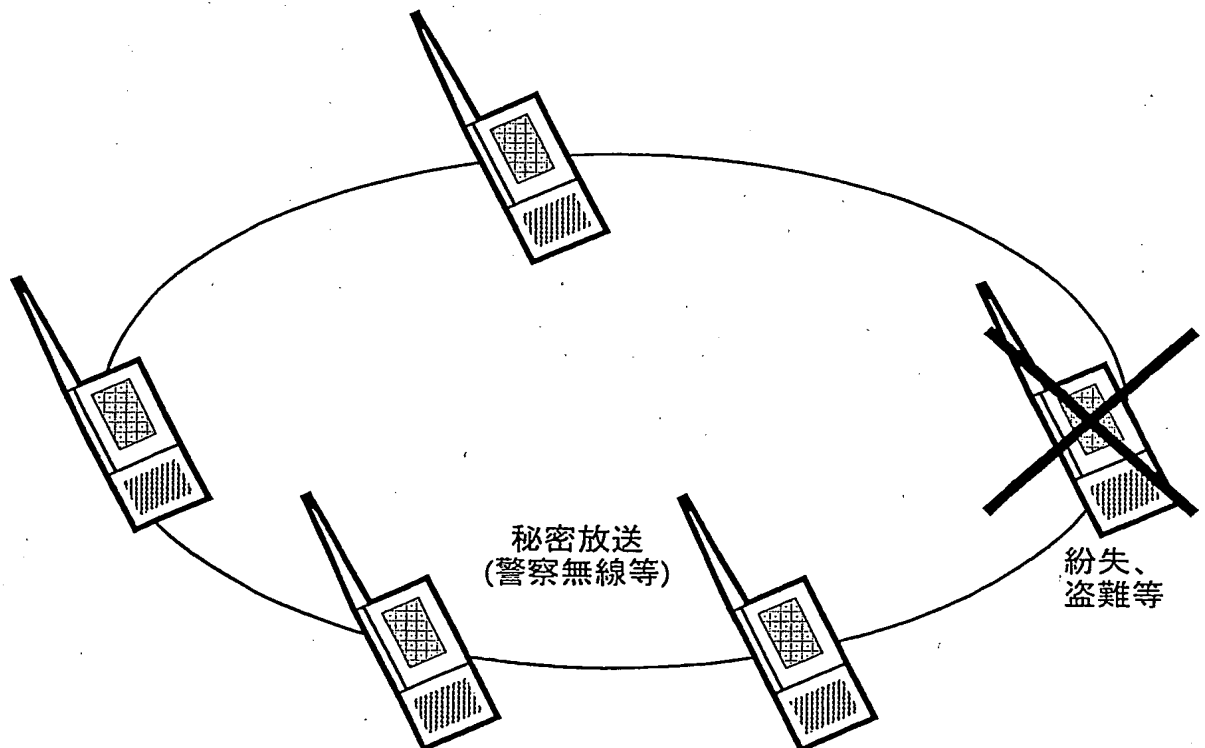
第 5 図

**THIS PAGE BLANK (USPTO)**

6/6



第 6 図



第 7 図

**THIS PAGE BLANK (USPTO)**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/05482

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-216766 A (Kabushiki Kaisha Kodo Ido Tsushin Security Gijutsu Kenkyusho), 04 August, 2000 (04.08.00), Par. Nos. [0029] to [0042] & WO 00/39957 A1 & EP 1059762 A1	1-14

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
28 July, 2003 (28.07.03)Date of mailing of the international search report  
12 August, 2003 (12.08.03)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**THIS PAGE BLANK (USPTO)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**